Claims:

1. A system for executing a software application comprising a plurality of hardware independent bytecodes, the system comprising:

a computing system that generates bytecodes;

a virtual machine, remote to the computing system, comprising means for receiving a plurality of bytecodes from said computing system, and means for executing said plurality of bytecodes;

means for testing said bytecodes against a set of predetermined criteria; and

means for securely distributing said testing means between said virtual machine and said computing system so that the bytecode verification completed by the computing system is authenticated by the virtual machine prior to the execution of the bytecodes by said virtual machine.

2. The system of Claim 1, wherein said remote computing system comprises means for determining that the bytecodes comply with a predetermined set of criteria to generate verified bytecodes, and means for generating a proof of authenticity attached to said verified bytecodes to generate authenticated bytecodes so that the authenticated bytecodes are tamper-resistant.

3. The system of Claim 2, wherein said virtual machine comprises means for determining that the authenticated bytecodes are not corrupted comprising means for generating a proof of authenticity based on the received bytecodes, and means for comparing said generated proof of authenticity against said authenticated bytecodes.

4. The system of Claim 2, wherein said virtual machine comprises means for performing limited run-time testing of said authenticated bytecodes.

5. The system of Claim 4, wherein said performing means comprises means for testing the memory access of said authenticated bytecodes.

6. The system of Claim 2, wherein said virtual machine comprises means for storing authenticated bytecodes in a non-volatile manner so that the authenticated bytecodes are not repeatedly communicated with the virtual machine.

7. A virtual machine for executing a software application comprising a plurality of bytecodes, the virtual machine being executed by a hardware processor, the virtual machine comprising:

means for receiving an authenticated bytecode, the authenticated bytecode being previously compared against a predetermined set of criteria and having a proof of authenticity;

means for determining that the authenticated bytecode is not corrupted based on the proof of authenticity; and

means for executing said bytecode.

8. The virtual machine of Claim 7 further comprising means for checking, at run-time, said authenticated bytecode for memory access errors.

9. The virtual machine of Claim 7, wherein said determining means comprises means for generating a proof of authenticity, and means for comparing the generated proof of authenticity against the proof of authenticity attached to the received bytecode.

10. The virtual machine of Claim 7, wherein said virtual machine comprises means for storing authenticated bytecodes in a non-volatile manner so that the authenticated bytecodes are not repeatedly communicated with the virtual machine.

11. A system for executing a software application comprising a plurality of bytecodes, the system comprising:

a computer system comprising means for verifying that a bytecode conforms to a predetermined set of criteria to generate a verified bytecode, and means for generating a secure verified bytecode from said verified bytecode; and

a virtual machine, remote from said computer system, for executing said secure verified bytecodes, said virtual machine comprising means for receiving said secure verified bytecodes, means for determining that the secure verified bytecodes are not corrupted, and means for executing said secure verified bytecodes.

12. The system of Claim 11, wherein said virtual machine comprises means for performing limited run-time testing of said received bytecodes.

13. The system of Claim 11, wherein said computing system comprises means for generating a proof of authenticity, and means for attaching said proof of authenticity to said bytecodes.

14. The system of Claim 12, wherein said virtual machine comprises means for generating a proof of authenticity, and means for comparing said generated proof of authenticity against said received proof of authenticity to determine that said received bytecode is not corrupted.

15. A smart card having a plastic card having a microcontroller embedded therein, the smart card comprising:

a virtual machine being executed by a microcontroller, the virtual machine executing a software application comprising a plurality of previously verified bytecodes, the virtual machine comprising means for receiving an authenticated bytecode, the authenticated bytecode being previously compared against a predetermined set of criteria and having a proof of authenticity, means for determining that the authenticated bytecode is not corrupted based on the proof of authenticity, and means for executing said bytecode.

16. The smart card of Claim 15 further comprising means for checking, at run-time, said received bytecode for run-time memory access errors.

17. The smart card of Claim 15, wherein said authenticated bytecode comprises a proof of authenticity attached to said received bytecode, and wherein said determining means

comprises means for generating a proof of authenticity, and means for comparing the generated proof of authenticity against the proof of authenticity attached to the received bytecode to determine if the authenticated bytecode is corrupted.

—

18. A method for executing a software application on a virtual machine, the application comprising a plurality of bytecodes, comprising:

receiving an authenticated bytecode by a virtual machine, the authenticated bytecode being previously compared against a predetermined set of criteria and having a proof of authenticity;

determining that the authenticated bytecode is not corrupted based on the proof of authenticity; and

executing said bytecode.

19. The virtual machine of Claim 18 further comprising checking, at run-time, said authenticated bytecode for memory access errors.

20. The virtual machine of Claim 18, wherein determining comprises generating a proof of authenticity, and comparing the generated proof of authenticity against the proof of authenticity attached to the received bytecode.

21. The virtual machine of Claim 18 further comprising storing authenticated bytecodes in a non-volatile manner so that the authenticated bytecodes are not repeatedly communicated with the virtual machine.

22. A virtual machine for executing a software application comprising a plurality of bytecodes, the virtual machine being executed by a hardware processor, the virtual machine comprising:

means for receiving data comprising a plurality of authenticated bytecodes, the authenticated bytecodes being previously compared against a predetermined set of criteria to reduce the amount of data received by the virtual machine;

means for determining that the authenticated bytecodes are not corrupted; and

means for executing said bytecodes.

23. The virtual machine of Claim 22, wherein said data received by said virtual machine excludes data used for verification of said bytecodes.